????

Harley Eades III

Computer Science
Augusta University
harley.eades@gmail.com

Abstract. TODO

1 Introduction

2 A Quaternary Semantics for SAND Attack Trees

Kordy et al. [1] gave a very elegant and simple semantics of attack-defense trees in boolean algebras. Unfortunately, while their semantics is elegant it does not capture the resource aspect of attack trees, it allows contraction, and it does not provide a means to model sequential conjunction. In this section we give a semantics of attack trees in the spirit of Kordy et al.'s using a four valued logic.

The propositional variables of our ternary logic, denoted by A, B, C, and D, range over the set $\{0, \frac{1}{4}, \frac{1}{2}, 1\}$. We think of 0 and 1 as we usually do in boolean algebras, but we think of $\frac{1}{4}$ and $\frac{1}{2}$ as intermediate values that can be used to break various structural rules. In particular we will use these values to prevent exchange for sequential conjunction from holding, and contraction from holding for parallel and sequential conjunction.

Definition 1. *The logical connectives of our four valued logic are defined as follows:*

Parallel Conjunction:

$$\begin{array}{l} A \odot_4 B = 1, \textit{where neither } A \textit{ nor } B \textit{ are } 0 \\ A \odot_4 B = 0, \textit{otherwise} \end{array}$$

Sequential Conjunction:

$$\begin{array}{l} \frac{1}{4} \rhd_4 B = \frac{1}{4}, \textit{where } B \neq 0 \\ A \rhd_4 B = \frac{1}{2}, \textit{where } A \in \{\frac{1}{2}, 1\} \textit{ and } B \neq 0 \\ A \rhd_4 B = 0, \textit{otherwise} \end{array}$$

Choice: $A \sqcup_4 B = \mathsf{max}(A, B)$

These definitions are carefully crafted to satisfy the necessary properties to model attack trees. Comparing these definitions with Kordy et al.'s [1] work we can see that choice is defined similarly, but parallel conjunction is not a product – ordinary conjunction – but rather a linear tensor product, and sequential conjunction is not actually definable in a boolean algebra, and hence, makes heavy use of the intermediate values to insure that neither exchange nor contraction hold. The following results solidify these claims.

We use the usual notion of equivalence between propositions, that is, propositions ϕ and ψ are considered equivalent, denoted by $\phi \equiv \psi$, if and only if they have the same truth tables. In order to model attack trees parallel conjunction must be symmetric, associative, but not satisfy contraction.

Lemma 1 (Parallel Conjunction is Symmetric). *For any A and B, $A \odot_4 B \equiv B \odot A$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 2 (Parallel Conjunction is Associative). *For any A, B, and C, $(A \odot_4 B) \odot_4 C \equiv A \odot_4 (B \odot_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 3 (Parallel Conjunction is not Contractive). *It is not the case that for any A, $A \odot_4 A \equiv A$.*

Proof. Suppose $A = \frac{1}{4}$. Then by definition $A \odot_4 A = 1$, but $\frac{1}{4}$ is not 1.

Similarly, sequential conjunction must be associative, but not symmetric nor satisfy contraction.

Lemma 4 (Sequential Conjunction is Associative). *For any A, B, and C, $(A \rhd_4 B) \rhd_4 C \equiv A \rhd_4 (B \rhd_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 5 (Sequential Conjunction is not Symmetric). *It is not the case that for any A and B, $A \rhd_4 B \equiv B \rhd_4 A$.*

Proof. Suppose $A = \frac{1}{4}$ and $B = \frac{1}{2}$. Then $A \rhd_4 B = \frac{1}{4}$, but $B \rhd_4 A = \frac{1}{2}$.

Lemma 6 (Sequential Conjunction is not Contractive). *It is not the case that for any A, $A \rhd_4 A \equiv A$.*

Proof. Suppose $A = 1$. Then by definition $A \odot A = \frac{1}{2}$, but $\frac{1}{2}$ is not 1.

Now choice satisfies all three properties, that is, it is symmetric, associative, and does satisfy contraction.

Lemma 7 (Choice is Symmetric). *For any A and B, $A \sqcup_4 B \equiv B \sqcup_4 A$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 8 (Choice is Associative). *For any A, B, and C, $(A \sqcup_4 B) \sqcup_4 C \equiv A \sqcup_4 (B \sqcup_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 9 (Choice is Contractive). *For any* A, $A \sqcup_4 A \equiv_4 A$.

Proof. This proof holds by simply comparing truth tables.

Finally, the necessary distributive laws hold.

Lemma 10 (Parallel Conjunction Distributes Over Choice).

i. For any A, B, *and* C, $A \odot_4 (B \sqcup_4 C) \equiv (A \odot_4 B) \sqcup_4 (A \odot_4 C)$.
ii. For any A, B, *and* C, $(A \sqcup_4 B) \odot_4 C \equiv (A \odot_4 C) \sqcup_4 (B \odot_4 C)$.

Proof. This proof holds by simply comparing truth tables.

Lemma 11 (Sequential Conjunction Distributes Over Choice).

i. For any A, B, *and* C, $A \rhd_4 (B \sqcup_4 C) \equiv (A \rhd_4 B) \sqcup_4 (A \rhd_4 C)$.
ii. For any A, B, *and* C, $(A \sqcup_4 B) \rhd_4 C \equiv (A \rhd_4 C) \sqcup_4 (B \rhd_4 C)$.

Proof. This proof holds by simply comparing truth tables.

At this point it is quite easy to model attack trees as formulas. The following defines their interpretation.

Definition 2. *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then we define the interpretation of* ATerms *to propositions as follows:*

$$\begin{array}{ll} [\![\mathbf{b} \in \mathbb{B}]\!] & = \alpha(\mathbf{b}) \\ [\![\mathsf{AND}\ T_1\ T_2]\!] & = [\![T_1]\!] \odot [\![T_2]\!] \\ [\![\mathsf{SAND}\ T_1\ T_2]\!] & = [\![T_1]\!] \rhd [\![T_2]\!] \\ [\![\mathsf{OR}\ T_1\ T_2]\!] & = [\![T_1]\!] \sqcup [\![T_2]\!] \end{array}$$

We can use this semantics to prove equivalences between attack trees.

Lemma 12 (Equivalence of Attack Trees in the Ternary Semantics). *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then for any attack trees* T_1 *and* T_2, $T_1 \approx T_2$ *if and only if* $[\![T_1]\!] \equiv [\![T_2]\!]$.

Proof. This proof holds by induction on the form of $T_1 \approx T_2$.

This is a very simple and elegant semantics, but it also leads to a more substantial theory.

References

1. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational aspects of attack–defense trees. In Pascal Bouvry, MieczysławA. Kłopotek, Franck Leprévost, Małgorzata Marciniak, Agnieszka Mykowiecka, and Henryk Rybiński, editors, *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103–116. Springer Berlin Heidelberg, 2012.

Appendix